

Section J

Attachment 3

“USCG Security Agreement”

ANNUAL COAST GUARD INFORMATION TECHNOLOGY CONTRACTOR USER SECURITY AGREEMENT

Date of Security Briefing: _____

As condition of being granted access to (system name) _____ located at
_____ via government contract number _____, delivery
order number (if applicable) _____, I agree to comply with the following Coast Guard
information technology user security requirements:

Unless specifically excepted in writing by contract or delivery order:

- I will comply with Coast Guard policies, regulations, and guidelines regarding access to, protection, handling, processing, transmission, distribution, and destruction of sensitive information (including but not limited to that designated "For Official Use Only" and "Classified"). This is to include, but not limited to, protection from unauthorized access, disclosure, modification, misuse, damage, or theft of information or information systems.
- I will not copy or remove copies of software licensed to Coast Guard without proper authorization nor will I import or use unauthorized software, firmware, or hardware in the work environment.
- I will protect all authentication devices (including but not limited to passwords) issued to me. I understand that password sharing or the use of another user's ID and password is prohibited. I will change my passwords when required by the system and whenever I suspect that they may have been compromised.
- I will report all security incidents, including password compromises, violations of software licensing agreements, and computer viruses, to the Coast Guard Information System Security Officer (ISSO) designated at the bottom of this form and to my employer.
- I will immediately notify the ISSO designated at the bottom of this form when I no longer require access to the network because of transfer, completion of project, etc., and of any changes in my work location or phone number.
- I will use any network connection for the processing, transmission, and storage of official U.S. Government-related or authorized work only.
- I will not knowingly introduce any malicious code into the network nor will I attempt to bypass or circumvent network security features or mechanisms.
- I will not relocate Coast Guard network equipment or software without proper authorization.
- Any computer and/or system connected to Coast Guard networks or systems shall be a standalone computer and/or system and shall not be connected to any other network, computer, or system without prior authorization.

I, the contractor employee/user, understand that failure to comply with any or all of the above security requirements could result in the loss of my system and/or network privileges and/or subject me to civil or criminal penalties.

PRINTED NAME OF CONTRACTOR EMPLOYEE/USER **COMPANY NAME**

SIGNATURE OF CONTRACTOR EMPLOYEE/USER **DATE SIGNED**

PRINTED NAME OF COAST GUARD ISSO **PHONE NUMBER OF COAST GUARD ISSO**

COAST GUARD INFORMATION TECHNOLOGY SECURITY CLAUSE

(a) No Contractor personnel shall commence any performance under this Task Order, requiring system access, until they:

(1) Have received a security briefing about the Automated Information Systems (AIS) Security Manual (COMDTINST M5500.13 (series)) from the appropriate Coast Guard Information Systems Security Officer (ISSO).

(2) Have signed an "Annual Coast Guard Information Technology Contractor User Security Agreement." A copy of this user security agreement is provided as Attached hereto. By signing the aforementioned user security agreement, the individual will be acknowledging their responsibility to properly use and safeguard all Coast Guard information technology resources and information related thereto. The COTR for this Task Order shall arrange the aforementioned security briefing.

(b) The Contractor shall access only those areas of Coast Guard information technology resources (e.g., computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, internet sites. etc.) explicitly stated in this Task Order and/or as approved by the COTR in writing as necessary for performance of the work under this Task Order. Any attempts by Contractor personnel to gain access to any information technology resources not explicitly authorized by the Performance Work Statement, other terms and conditions in this Task Order, or approved in writing by the COTR is strictly prohibited. In the event of violation of this provision, the Coast Guard will take appropriate action with regard to the Task Order.

(c) Contractor access to Coast Guard computer systems and/or networks from a remote location is a temporary privilege for the mutual convenience it offers while the Contractor performs business for the Coast Guard. It is not a right, a guarantee, a condition of the Task Order, nor is it Government Furnished Equipment (GFE).

(d) Contractor access may be terminated for unauthorized use. The Contractor agrees to hold the Coast Guard harmless and the Contractor will not request additional time or money under the Task Order for delay resulting from unauthorized use.